UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,684	08/31/2001	Guy Eden	SLA 1086	2139

55286   7590   08/07/2007
SHARP LABORATORIES OF AMERICA, INC.
C/O LAW OFFICE OF GERALD MALISZEWSKI
P.O. BOX 270829
SAN DIEGO, CA 92198-2829

EXAMINER
HA, LEYNNA A

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
08/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _22 May 2007_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1,2,4-14 and 16-27_ is/are pending in the application.

    4a) Of the above claim(s) _3 and 15_ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-2, 4-14, and 16-27_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-2, 4-14, and 16-27 are pending.

Applicant cancels claims 3 and 15.

Response to Arguments

2.   **Applicant's arguments filed 5/22/2007 have been fully considered but they are not persuasive.**

Examiner traverses the argument (pg.12) that Dutta is silent on the profile that includes an address field and an encryption field and unable to select the type of encryption that is used. Seder suggests selecting a profile in terms of the printed documents may convey or point to the database records containing encryption keys (Seder - col.6, lines 18-20). This obviously reads on encrypting the scanned document in response to the encryption field of the selected profile because the proper keys of the intended recipient (destination) will be able to decrypt and view the document. Seder also discloses using the identifier to access one or more database records corresponding to the document (Seder - c ol.4, lines 63-66). Databases of records are obviously for populating and for querying files/records stored therein. Thus, being able to access the database records obviously suggests the ability to select a profile from the directory. Seder suggests encrypting the scanned document, selecting a document/profile, and a specified link is embedded in the electronic version of the document stored in a database record associated with that document (Seder - col.4,

lines 28-47), but Dutta is combined to explain the encryption is in response to the

encryption field and sending the encrypted document in response to the address field.

Dutta discloses an invention that provides security and privacy benefits to both senders

and recipients while providing delivery of a parcel or physical document. The recipient's

address is in encrypted form is printed on the envelope [Dutta - 0004]. Dutta teaches

providing secure delivery of a parcel or document by using encryption to shield a

recipient's address, or a sender's address, or both [Dutta - 0015]. To guide the

envelope through routing and delivery, conventional scanner is used to read the data

displayed on the envelope [0016] and may retrieve a private key from a secure key

database through a secure key manager module [Dutta - 0017-0018]. Dutta teaches

the keys are used to encrypt data and decrypts the encrypted data to yield the

recipient's address [Dutta - 0030, 0036, and 0042]. The claimed encryption field can

broadly be Dutta's encryption key, which obviously suggests the encryption used for the

particular document. Hence, the key and a person's address obviously suggest a

profile(s) of the document corresponding to the encryption field and address for secure

delivery and routing purposes.

As such, examiner traverses argument on page 13, that Seder and Dutta

combination fail to disclose the claimed invention because it would have been obvious

for a person of ordinary skills in the art to combine Seder with Dutta to teach encrypting

the scanned document in response to the encryption field of the selected profile and

sending the encrypted document to a destination, in response to the address field of the

selected profile would be for security reasons [Dutta - 0018] of delivery and routing

purposes [Dutta - 0004], the use of encryption shields a recipient's/sender's address

[Dutta - 0015] which is in response to the address of the selected profile in order to

decrypt the encrypted data to yield recipient's address [Dutta - 0030].

Examiner is not relying on merely the knowledge of a person of ordinary skills in

the art to supply the motivation because examiner have provided the citation where

Dutta teaches the motivation of secure delivery and routing purposes [Dutta – 0004,

0018] utilizing the encryption field and address field [Dutta – 0015, 0030] of the

document/profile [Dutta – 0036, 0042].

Examiner traverses the argument (pg.14-16) that Hind does not disclose the use

of profiles, profile address fields, and sending the scanned document in response to

selecting the profile from a directory because it has been established that the Seder and

Dutta combination have met these limitations. Hind is brought forth to teach the

certificate authority because it would have been obvious for a person of ordinary skills in

the art at the time of the invention to combine the Seder and Dutta combination with

Hind teaching a signed document by the Certification Authority in order to verify the

authenticity of the document (Hind - col.9, lines 45-53 and col.11, lines 35-38). The

motivation again is not based on assumption because examiner provided the citation

where Hind teaches the motivation.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or
> described as set forth in section 102 of this title, if the differences between the subject
> matter sought to be patented and the prior art are such that the subject matter as a whole
> would have been obvious at the time the invention was made to a person having ordinary
> skill in the art to which said subject matter pertains. Patentability shall not be negatived by
> the manner in which the invention was made.

3.   **Claims 1-2, 4-9, 11-14, and 16-23, 25-27 are rejected under 35 U.S.C. 103(a)**

as being obvious over Seder, et al. (US 6,401,097), and further in view of Dutta

(US 2002/0138759 A1).

As per claim 1:

Seder discloses in a digital scanner, a method for secure document transmission

the method comprising:

creating computer text files, called profiles, in a directory of a scanner device

(col.2, lines 63-67; Seder discloses a record may include meta-data associated

with the document that is stored in a database refers to the claimed text files or

profiles in a directory.),

storing the profiles in a directory; **(col.4, lines 48-53 and 63-65)**

at a scanner device user interface, selecting a profile from the directory; **(col.4,**

lines 52-65 and col.6, lines 8-12)

accepting a physical medium document; **(col.5, line 62)**

scanning a document; **(col.5, lines 35-36)**

Seder discloses a record may include meta-data associated with the document that is stored in a database wherein the record refers to the claimed text files or profiles and the database refers to the claimed directory (col.2, lines 63-67). The database stores different forms of information that makes up the claimed profile (record) and not just meta-data. For instance, Seder discloses specifying the path (electronic address) and file to be associated with that text. The specified link is embedded in the electronic version of the document where such links can be sensed and stored in a database record associated with that document (col.4, lines 28-47). This clearly proves that Seder is teaching a network address rather than the address of a location in a memory is sent to a destination according to the selected profile in the database (col.4, lines 40-53). Seder further discloses the scanned document to have a watermark (col.5, lines 33-34) that identifies the document (col.4, lines 56-59) and to encrypt an electronic version of the file (scanned document) and an encoding key in a watermark in the printed document (or in a database record identified by the watermark) (col.6, lines 8-13). Seder discusses the printed documents may convey or point to the database records containing encryption keys (col.6, lines 18-20). This obviously reads on the encrypting the scanned document in response to the encryption field of the selected profile because the proper keys of the intended recipient (destination) will be able to decrypt and view the document. However, Seder did not include each profile having an address field and an encryption field; encrypting the scanned document in response to the encryption field of the selected profile; and, sending the encrypted document to a destination, in response to the address field of the selected profile.

Dutta discloses an invention that provides security and privacy benefits to both

senders and recipients while providing delivery of a parcel or physical document. The

recipient's address is in encrypted form is printed on the envelope [0004]. Dutta

discloses envelope refers to the claimed Dutta teaches providing secure delivery of a

parcel or document by using encryption to shield a recipient's address, or a sender's

address, or both [0015]. To guide the envelope through routing and delivery,

conventional scanner is used to read the data displayed on the envelope [0016] and

may retrieve a private key from a secure key database through a secure key manager

module [0017-0018]. Dutta teaches the keys are used to encrypt data and decrypts the

encrypted data to yield the recipient's address [0030, 0036, and 0042]. Hence, the

encryption field and an address field obviously disclose profile(s) of the document

corresponding to the person's address for delivery and routing purposes.

Therefore, it would have been obvious for a person of ordinary skills in the art to

combine Seder with the teaching each profile having an address field and an

encryption field; encrypting the scanned document in response to the encryption field

of the selected profile; and, sending the encrypted document to a destination, in

response to the address field of the selected profile as taught by Dutta because for

security reasons [0018] of delivery and routing purposes [0004], the use of encryption

shields a recipient's/sender's address [0015] which is in response to the address of the

selected profile in order to decrypt the encrypted data to yield recipient's address

[0030].

As per claim 2: **See Dutta on [0018 and 0030];** discusses sending the encrypted document to the destination includes sending the encrypted document in response to the address field of the selected profile.

As per claim 3: **Cancelled**

As per claim 4: **See Dutta on [0017-0018 and 0030];** discusses assigning each profile to a corresponding destination; and, wherein selecting a profile includes: selecting a destination; and, using the profile assigned to the selected destination.

As per claim 5: **See Seder on col.1, lines 61-62;** discusses selecting a profile includes selecting a profile having an address selected from the group including email addresses and file transfer protocol (FTP) addresses.

As per claim 6: **See Dutta on [0017-0018];** discusses selecting a profile having an encryption field selected from the group including symmetric and asymmetric (public) keys.

As per claim 7: **See Dutta on [0017-0018];** discusses selecting a profile having an asymmetric key; and, wherein creating profiles includes storing public keys in the created profiles.

As per claim 8: **See Dutta on [0017-0018 and 0030];** discusses selecting a profile having a symmetric key; and, wherein creating profiles includes storing symmetric keys in the created profiles.

As per claim 9: **See Dutta on [0017-0018 and 0030];** discusses generating a plurality of passwords for the corresponding plurality of user groups; and wherein

storing the profiles in a directory includes storing profiles in a profile directory, in

response to the generated password.

As per claim 11: See Seder on col.6, lines 18-23 and Dutta on [0017-0018 and

0030]; discusses generating a random session key; encrypting the document with the

session key using a symmetric algorithm, encrypting the session key with an

asymmetric algorithm using the selected profile public key, and wherein sending the

encrypted document to the address from the selected profile includes sending the

encrypted session key.

As per claim 12: See Dutta on [0017-0018 and 0030]; discusses creating profiles

includes creating a profile with a plurality of addresses and a corresponding plurality of

public keys, wherein encrypting the document includes generating a single encrypted

document using an asymmetric algorithm, and wherein sending the encrypted

document includes sending the single encrypted document to each of the plurality of

addresses in the profile.

As per claim 13:

Seder discloses in a digital scanner, a method for secure document transmission

the method comprising:

storing computer text files, called profiles, in a directory of a scanner device

(col.2, lines 63-67; Seder discloses a record may include meta-data associated

with the document that is stored in a database refers to the claimed text files or

profiles in a directory.);

at a user interface associated with the scanner device, selecting a profile from

the directory; **(col.4, lines 48-53 and 63-65)**

scanning a document; **(col.5, lines 35-36)**

Seder discloses a record may include meta-data associated with the document

that is stored in a database wherein the record refers to the claimed text files or profiles

and the database refers to the claimed directory (col.2, lines 63-67). The database

stores different forms of information that makes up the claimed profile (record) and not

just meta-data. For instance, Seder discloses specifying the path (electronic address)

and file to be associated with that text. The specified link is embedded in the electronic

version of the document where such links can be sensed and stored in a database

record associated with that document (col.4, lines 28-47). This clearly proves that

Seder is teaching a network address rather than the address of a location in a memory

is sent to a destination according to the selected profile in the database (col.4, lines 40-

53). Seder further discloses the scanned document to have a watermark (col.5, lines

33-34) that identifies the document (col.4, lines 56-59) and to encrypt an electronic

version of the file (scanned document) and encode an encoding key in a watermark in

the printed document (or in a database record identified by the watermark) (col.6, lines

8-13). Seder discusses the printed documents may convey or point to the database

records containing encryption keys (col.6, lines 18-20). This obviously reads on the

encrypting the scanned document in response to the encryption field of the selected

profile because the proper keys of the intended recipient (destination) will be able to

decrypt and view the document. However, Seder did not include each profile having an

address field and an encryption field; encrypting the scanned document in response to the encryption field of the selected profile; and, sending the encrypted document to a destination, in response to the address field of the selected profile.

Dutta discloses an invention that provides security and privacy benefits to both senders and recipients while providing delivery of a parcel or physical document. The recipient's address is in encrypted form is printed on the envelope [0004]. Dutta discloses envelope refers to the claimed Dutta teaches providing secure delivery of a parcel or document by using encryption to shield a recipient's address, or a sender's address, or both [0015]. To guide the envelope through routing and delivery, conventional scanner is used to read the data displayed on the envelope [0016] and may retrieve a private key from a secure key database through a secure key manager module [0017-0018]. Dutta teaches the keys are used to encrypt data and decrypts the encrypted data to yield the recipient's address [0030, 0036, and 0042]. Hence, the encryption field and an address field obviously disclose profile(s) of the document corresponding to a person's address for delivery and routing purposes.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Seder with the teaching each profile having an address field and an encryption field; encrypting the scanned document in response to the encryption field of the selected profile; and, sending the encrypted document to a destination, in response to the address field of the selected profile as taught by Dutta because for security reasons [0018] of delivery and routing purposes [0004], the use of encryption shields a

recipient's/sender's address [0015] which is in response to the address of the selected

profile in order to decrypt the encrypted data to yield recipient's address [0030].

As per claim 14:

Seder discloses in a digital scanner, a method for secure document transmission

the method comprising:

a profile directory having a user interface for selecting computer text files, called

profiles **(col.2, lines 63-67; Seder discloses a record may include meta-data**

associated with the document that is stored in a database refers to the claimed

text files or profiles in a directory.);

a document scanner to accept physical medium documents, create scanned

documents **(col.5, lines 35-36).**

Seder discloses a record may include meta-data associated with the document

that is stored in a database wherein the record refers to the claimed text files or profiles

and the database refers to the claimed directory (col.2, lines 63-67). The database

stores different forms of information that makes up the claimed profile (record) and not

just meta-data. For instance, Seder discloses specifying the path (electronic address)

and file to be associated with that text. The specified link is embedded in the electronic

version of the document where such links can be sensed and stored in a database

record associated with that document (col.4, lines 28-47). This clearly proves that

Seder is teaching a network address rather than the address of a location in a memory

is sent to a destination according to the selected profile in the database (col.4, lines 40-

53). Seder further discloses the scanned document to have a watermark (col.5, lines

33-34) that identifies the document (col.4, lines 56-59) and to encrypt an electronic

version of the file (scanned document) and encode an encoding key in a watermark in

the printed document (or in a database record identified by the watermark) (col.6, lines

8-13). Seder discusses the printed documents may convey or point to the database

records containing encryption keys (col.6, lines 18-20). This obviously reads on the

encrypting the scanned document in response to the encryption field of the selected

profile because the proper keys of the intended recipient (destination) will be able to

decrypt and view the document. However, Seder did not include each profile having an

address field and an encryption field; encrypting the scanned document in response to

the encryption field of the selected profile; and, sending the encrypted document to a

destination, in response to the address field of the selected profile.

Dutta discloses an invention that provides security and privacy benefits to both

senders and recipients while providing delivery of a parcel or physical document. The

recipient's address is in encrypted form is printed on the envelope [0004]. Dutta

discloses envelope refers to the claimed Dutta teaches providing secure delivery of a

parcel or document by using encryption to shield a recipient's address, or a sender's

address, or both [0015]. To guide the envelope through routing and delivery,

conventional scanner is used to read the data displayed on the envelope [0016] and

may retrieve a private key from a secure key database through a secure key manager

module [0017-0018]. Dutta teaches the keys are used to encrypt data and decrypts the

encrypted data to yield the recipient's address [0030, 0036, and 0042]. Hence, the

encryption field and an address field obviously disclose profile(s) of the document corresponding to the person's address for delivery and routing purposes.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Seder with the teaching each profile having an address field and an encryption field; encrypting the scanned document in response to the encryption field of the selected profile; and, sending the encrypted document to a destination, in response to the address field of the selected profile as taught by Dutta because for security reasons [0018] of delivery and routing purposes [0004], the use of encryption shields a recipient's/sender's address [0015] which is in response to the address of the selected profile in order to decrypt the encrypted data to yield recipient's address [0030].

As per claim 15: **Cancelled**

As per claim 16: **See Seder on col.4, lines 28-33 and Dutta on [0017-0018 and 0030];** discusses a memory for storing the profiles; and wherein the profile directory has an interface for creating profiles having an address field and an encryption field.

As per claim 17: **See Seder col.1, lines 61-62;** discusses selecting a profile includes selecting a profile having an address selected from the group including email addresses and file transfer protocol (FTP) addresses.

As per claim 18: **See Seder col.1, lines 61-62;** discusses selecting a profile includes selecting a profile having an address selected from the group including email addresses and file transfer protocol (FTP) addresses.

As per claim 19: **See Dutta on [0017-0018];** discusses the profile directory, and

further Seder discusses creating profiles having an address field and an encryption field including symmetric and asymmetric (public) keys.

As per claim 20:   See Dutta on [0017-0018];discusses the memory stores the public keys corresponding to each profile.

As per claim 21: See Dutta on [0017-0018 and 0030];discusses creating profiles having an address field and an encryption field wherein the memory stores the symmetric keys corresponding to each profile.

As per claim 22:   See Seder on col.4, lines 8-10 and 63-62; discusses the profile directory, and an interface for generating passwords.

As per claim 24: Seder discusses the document scanner generates a random session key and encrypts the document with the session key using a symmetric algorithm; **(col.6, lines 8-16)** wherein the document scanner encrypts the session key with an asymmetric algorithm using the selected profile public key; and, **(col.6, lines 18-23)** wherein the network interface transmits the encrypted session key with the encrypted document. **(col.6, line 62 – col.6, line 2)**

As per claim 25: Seder the profile directory supplies a selected profile with a plurality of addresses and a corresponding plurality of public keys; **(col.6, lines 22-23)** wherein the document scanner encrypts the document into a single encrypted document using an asymmetric algorithm; and **(col.6, lines 8-10)** wherein the network interface sends the single encrypted document to each of the plurality of addresses in the selected profile. **(col.4, lines 28-33)**

As per claim 26:

Seder discloses a digital scanner secure document transmission system, the

system comprising:

a directory **(col.2, lines 63-67; Seder discloses a record may include meta-**

data associated with the document that is stored in a database refers to the

claimed text files or profiles in a directory.) having a user interface for selecting

(col.6, lines 8-12) an address field **(col.4, lines 27-37)**

a document scanner to accept physical medium document **(col.5, lines 62)**,

create a scanned document **(col.5, lines 35-36)**, and encrypt the scanned document

using the cross-referenced generation field; and, **(col.6, lines 8-13 and 18-20)**

Seder discloses a record may include meta-data associated with the document

that is stored in a database wherein the record refers to the claimed text files or profiles

and the database refers to the claimed directory (col.2, lines 63-67). The database

stores different forms of information that makes up the claimed profile (record) and not

just meta-data. For instance, Seder discloses specifying the path (electronic address)

and file to be associated with that text. The specified link is embedded in the electronic

version of the document where such links can be sensed and stored in a database

record associated with that document (col.4, lines 28-47). This clearly proves that

Seder is teaching a network address rather than the address of a location in a memory

is sent to a destination according to the selected profile in the database (col.4, lines 40-

53). Seder further discloses the scanned document to have a watermark (col.5, lines

33-34) that identifies the document (col.4, lines 56-59) and to encrypt an electronic

version of the file (scanned document) and encode an encoding key in a watermark in

the printed document (or in a database record identified by the watermark) (col.6, lines

8-13). Seder discusses the printed documents may convey or point to the database

records containing encryption keys (col.6, lines 18-20). This obviously reads on the

encrypting the scanned document in response to the encryption field of the selected

profile because the proper keys of the intended recipient (destination) will be able to

decrypt and view the document. However, Seder did not include each profile having an

address field and an encryption field; encrypting the scanned document in response to

the encryption field of the selected profile; and, sending the encrypted document to a

destination, in response to the address field of the selected profile.

Dutta discloses an invention that provides security and privacy benefits to both

senders and recipients while providing delivery of a parcel or physical document. The

recipient's address is in encrypted form is printed on the envelope [0004]. Dutta

discloses envelope refers to the claimed Dutta teaches providing secure delivery of a

parcel or document by using encryption to shield a recipient's address, or a sender's

address, or both [0015]. To guide the envelope through routing and delivery,

conventional scanner is used to read the data displayed on the envelope [0016] and

may retrieve a private key from a secure key database through a secure key manager

module [0017-0018]. Dutta teaches the keys are used to encrypt data and decrypts the

encrypted data to yield the recipient's address [0030, 0036, and 0042]. Hence, the

encryption field and an address field obviously disclose profile(s) of the document

corresponding to the person's address for delivery and routing purposes.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Seder with the teaching each profile having an address field and an encryption field; encrypting the scanned document in response to the encryption field of the selected profile; and, sending the encrypted document to a destination, in response to the address field of the selected profile as taught by Dutta because for security reasons [0018] of delivery and routing purposes [0004], the use of encryption shields a recipient's/sender's address [0015] which is in response to the address of the selected profile in order to decrypt the encrypted data to yield recipient's address [0030].

As per claim 27:

Seder discloses in a digital scanner, a method for secure document transmission, the method comprising:

storing the cross-referenced fields in a directory; **(col.2, lines 63-67 and col.4, lines 48-53 and 63-65; Seder discloses a record may include meta-data associated with the document that is stored in a database refers to the claimed text files or profiles in a directory.)**

at a scanner device user interface, selecting an address from

the directory; **(col.4, lines 52-65 and col.6, lines 8-12)**

accepting a physical medium document; **(col.5, lines 62)**

scanning the document; **(col.5, lines 35-36)**

encrypting the scanned document using the cross-referenced

encryption field; and **(col.6, lines 8-13 and 18-20)**

Seder discloses a record may include meta-data associated with the document

that is stored in a database wherein the record refers to the claimed text files or profiles

and the database refers to the claimed directory (col.2, lines 63-67). The database

stores different forms of information that makes up the claimed profile (record) and not

just meta-data. For instance, Seder discloses specifying the path (electronic address)

and file to be associated with that text. The specified link is embedded in the electronic

version of the document where such links can be sensed and stored in a database

record associated with that document (col.4, lines 28-47). This clearly proves that

Seder is teaching a network address rather than the address of a location in a memory

is sent to a destination according to the selected profile in the database (col.4, lines 40-

53). Seder further discloses the scanned document to have a watermark (col.5, lines

33-34) that identifies the document (col.4, lines 56-59) and to encrypt an electronic

version of the file (scanned document) and encode an encoding key in a watermark in

the printed document (or in a database record identified by the watermark) (col.6, lines

8-13). Seder discusses the printed documents may convey or point to the database

records containing encryption keys (col.6, lines 18-20). This obviously reads on the

encrypting the scanned document in response to the encryption field of the selected

profile because the proper keys of the intended recipient (destination) will be able to

decrypt and view the document. However, Seder did not include each profile having an

address field and an encryption field; encrypting the scanned document in response to

the encryption field of the selected profile; and, sending the encrypted document to a

destination, in response to the address field of the selected profile.

Dutta discloses an invention that provides security and privacy benefits to both senders and recipients while providing delivery of a parcel or physical document. The recipient's address is in encrypted form is printed on the envelope [0004]. Dutta discloses envelope refers to the claimed Dutta teaches providing secure delivery of a parcel or document by using encryption to shield a recipient's address, or a sender's address, or both [0015]. To guide the envelope through routing and delivery, conventional scanner is used to read the data displayed on the envelope [0016] and may retrieve a private key from a secure key database through a secure key manager module [0017-0018]. Dutta teaches the keys are used to encrypt data and decrypts the encrypted data to yield the recipient's address [0030, 0036, and 0042]. Hence, the encryption field and an address field obviously disclose profile(s) of the document corresponding to the person's address for delivery and routing purposes.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Seder with the teaching each profile having an address field and an encryption field; encrypting the scanned document in response to the encryption field of the selected profile; and, sending the encrypted document to a destination, in response to the address field of the selected profile as taught by Dutta because for security reasons [0018] of delivery and routing purposes [0004], the use of encryption shields a recipient's/sender's address [0015] which is in response to the address of the selected profile in order to decrypt the encrypted data to yield recipient's address [0030].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.   **Claims 10 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over the Seder and Dutta combination, and further in view of Hind, et al. (US 6,980,660).**

As per claim 10:

The Seder discusses selecting a profile and storing a public key (col.6, lines 18-23) and wherein encrypting the document using the encryption field (col.4, lines 56-57) from the selected profile includes using the public key to encrypt the document. (col.6, lines 8-13). Seder discusses the digital signature generated from an electronic document can be encoded in a printed document as the payload of an embedded watermark, or can be included in a database record identified by the watermark (col.5, lines 61-64). The Seder and Dutta combination teaches encrypting the scanned document in response to the encryption field of the selected profile and, sending the encrypted document to a destination, in response to the address field of the selected profile. However, fails to include the certification authority.

Hind discloses implements security such as authentication and encryption that includes cryptography keys to determine the access privileges (col.7, lines 2-35).

Further, Hind uses the Certificate Authority to verify the authenticity of the signature and

a public key (col.9, lines 45-53 and col.11, lines 35-38).

Therefore, it would have been obvious for a person of ordinary skills in the art at

the time of the invention to include with the encryption of the document by using the

public key as taught by Seder signed by the certification authority as taught by Hind

because the Certification Authority verifies the authenticity of the document.

As per claim 23:

The Seder discusses selecting a profile and storing a public key (col.6, lines 18-

23) and wherein encrypting the document using the encryption field (col.4, lines 56-57)

from the selected profile includes using the public key to encrypt the document. (col.6,

lines 8-13). Seder discusses the digital signature generated from an electronic

document can be encoded in a printed document as the payload of an embedded

watermark, or can be included in a database record identified by the watermark (col.5,

lines 61-64). The Seder and Dutta combination teaches encrypting the scanned

document in response to the encryption field of the selected profile and, sending the

encrypted document to a destination, in response to the address field of the selected

profile. However, fails to include the certification authority.

Hind discloses implements security such as authentication and encryption that

includes cryptography keys to determine the access privileges (col.7, lines 2-35).

Further, Hind uses the Certificate Authority to verify the authenticity of the signature and

a public key and that the fields of the certificate may contain information where access

is granted or denied based on the locally obtained information (col.9, lines 45-53 and

col.11, lines 35-38).

Therefore, it would have been obvious for a person of ordinary skills in the art at

the time of the invention to include with the encryption of the document by using the

public key as taught by Seder signed by the certification authority as taught by Hind

because the Certification Authority verifies the authenticity of the document (Hind -

col.9, lines 45-53 and col.11, lines 35-38).

Conclusion

5.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire

THREE MONTHS from the mailing date of this action. In the event a first reply

is filed within TWO MONTHS of the mailing date of this final action and the

advisory action is not mailed until after the end of the THREE-MONTH

shortened statutory period, then the shortened statutory period will expire on

the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In

no event, however, will the statutory period for reply expire later than SIX

MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-

3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR

only. For more information about the PAIR system, see http://pair-direct.uspto.gov.

Should you have questions on access to the Private PAIR system, contact the

Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like

assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100